

On the Existence of Absolutely Maximally Entangled States of Minimal Support

Antonio Bernal*

Department de Matemàtiques i Informàtica. Universitat de Barcelona

May 3, 2016

Abstract

In this paper we prove that no absolutely maximally entangled, AME, state with minimal support exists with 7 sites and 5 levels.

General AME states are pure multipartite states that, when reduced to half or less of the sites, the maximum entropy mixed state is obtained. They have found applications in teleportation and quantum secret sharing, and finding conditions for their existence is a well known open problem. We consider the version of this problem for minimally supported AME states. We single out known both sufficient and necessary conditions in that case. From our negative result, we show that the necessary condition is not sufficient. The proof uses a recent result on the theory of general, nonlinear, classical codes.

1 Introduction

In this paper we consider pure states of n qudrits, $|\Psi\rangle \in (\mathbb{C}^d)^{\otimes n}$, such that, when tracing out half or more of the sites, the mixed state of maximum confusion is obtained. Those states have been called absolutely maximally entangled, AME, or $AME(n, d)$, in [3] in the context of quantum secret sharing schemes. The same concept had already appeared in [6] in the context of quantum error correcting codes, under the term “ $\lfloor n/2 \rfloor$ -uniform”.

AME states have found applications in fields like teleportation or quantum secret sharing, and provide links between different areas of mathematics, like coding theory, orthogonal arrays, quantum error correcting codes or combinatorial designs, see [2], [3] and [4].

A well known open problem is to determine conditions for the existence of AME states. This paper deals with the problem of existence of AME states that are supported on a minimal set of kets from the computational basis.

*Electronic address: abernal@ub.edu
Supported by project FIS2013-41757-P

For AME states of minimal support, a necessary condition is that $d \geq \lceil n/2 \rceil + 1$ if $n \geq 4$ and d is any integer [2], and a sufficient condition is that $d \geq n - 1$, when d is a prime power, [1, 2, 4].

We prove that there is no $AME(7, 5)$ state with minimal support. The result is proved using the standard theory of linear codes, along with a recent result that relates linear and nonlinear codes, see [5]. Since the case where $n = 7$ and $d = 5$ is not forbidden by the above necessary condition, we see that the condition is not sufficient.

The organization of the paper is as follows. Sections 2 and 3 are devoted to review the general definitions and both necessary and sufficient conditions. In section 4, it is proved that no $AME(7, 5)$ states of minimal support exist. Section 5 contains concluding remarks and some open questions.

2 Absolutely maximally entangled states

Let n and d be integers $n, d \geq 2$. Let $|\Psi\rangle$ be a pure multipartite state on n sites, where the local Hilbert space is d -dimensional. That is, $|\Psi\rangle \in (\mathbb{C}^d)^{\otimes n}$.

Definition 1. We say that $|\Psi\rangle$ is absolutely maximally entangled with n sites and local dimension d , $AME(n, d)$, if for any partition of $\{1, \dots, n\}$ into two disjoint subsets A and B , with $|B| = m \leq |A| = n - m$, the density obtained from $|\Psi\rangle\langle\Psi|$ tracing out the sites on the entries in A is multiple of the identity,

$$\text{Tr}_A |\Psi\rangle\langle\Psi| = \frac{1}{d^m} \text{Id}_{\mathbb{C}^{\otimes m}}.$$

If V is a vector space $v \in V$ and $\mathcal{B} \subset V$ is a basis of V , the support of v in the basis \mathcal{B} is the number of nonzero coordinates of v in the basis \mathcal{B} .

A linear algebra argument shows that any $AME(n, d)$ state has support on the computational basis of at least $d^{\lfloor n/2 \rfloor}$.

Definition 2. Given two integers n, d , with $n, d \geq 2$, we will say that an $AME(n, d)$ state $|\Psi\rangle$ is of minimal support if the support of $|\Psi\rangle$ in the computational basis is $d^{\lfloor n/2 \rfloor}$.

There is a characterization of $AME(n, d)$ states of minimal support in terms of classical codes.

We consider the set $\mathbb{Z}_d = \{0, \dots, d - 1\}$. A code over the alphabet \mathbb{Z}_d of wordlength n is a subset $\mathcal{C} \subset \mathbb{Z}_d^n$. On \mathcal{C} we consider the Hamming distance. Given two words $w, w' \in \mathcal{C}$, the Hamming distance between w and w' , $D_H(w, w')$ is the number of coordinates on which the words w and w' differ. The minimum distance δ of the code \mathcal{C} is the minimum of the distances $D_H(w, w')$ between different words $w, w' \in \mathcal{C}$. The well known Singleton bound establishes that $|\mathcal{C}| \leq d^{n-\delta+1}$. A code is called maximum distance separable, MDS, if the singleton bound is an equality. See [7] for general properties of codes.

Theorem 1 ([2, 4]). The existence of $AME(n, d)$ of minimal support is equivalent to the existence of MDS codes of wordlength n , alphabet size d and minimum distance $\lceil n/2 \rceil + 1$. The words of the code and the kets of the state are in one onto one correspondence.

The following property follows by a combinatorial argument involving the associated MDS code.

Proposition 1 ([2]). *Let $n \geq 3$ be an integer. If there is an $AME(n, d)$ state of minimal support, then there is an $AME(n-1, d)$ state of minimal support.*

So, given d , the set of all n such that $AME(n, d)$ states of minimal support exist is an interval.

Corollary 1. *For any integer $d \geq 2$, there is an integer $\mathcal{N}(d)$ such that, an $AME(n, d)$ state of minimal support exists if, and only if, $n \leq \mathcal{N}(d)$.*

We finally mention the necessary condition for the existence of AME states of minimal support:

Theorem 2 ([2]). *If $n \geq 4$ and an $AME(n, d)$ state of minimal support exists, then $d \geq \lceil \frac{n}{2} \rceil + 1$.*

This condition forbids many combinations (n, d) for possible $AME(n, d)$ states of minimal support. For example, although $AME(6, 2)$ states exist, none of them can be of minimal support, [2].

Theorem 2 can be read as an upper bound for $\mathcal{N}(d)$.

Corollary 2. *For any integer $d \geq 3$, $\mathcal{N}(d) \leq 2d - 2$, if $\mathcal{N}(d)$ is even, and $\mathcal{N}(d) \leq 2d - 3$, if $\mathcal{N}(d)$ is odd.*

Proof. We observe that theorem 2 is true when $d \geq 3$, for any $n \geq 2$, the cases not covered in theorem 2 being trivial. Since $AME(\mathcal{N}(d), d)$ states of minimal support exist, the statement is another way to write the inequality $\lceil \mathcal{N}(d)/2 \rceil + 1 \leq d$. \square

The results discussed so far are true for general integer values of the local dimension d .

3 Using linear MDS codes

In the case where d is a prime power, the alphabet $\{0, \dots, d-1\}$ can be given a unique field structure, $GF(d)$. In this case, there is more detailed information on certain cases.

In the case of linear $MDS[n, k]$ codes over the field $GF(d)$, where n stands for the code length and k is the code dimension, the Singleton identity reads

$$k = n - \delta + 1,$$

where δ is the minimum distance. The linear MDS codes that give rise to $AME(n, d)$ states of minimal support have, according to the Singleton identity and theorem 1, dimension $k = \lfloor n/2 \rfloor$.

When d is the power of a prime number, we have the theory of generalized Reed Solomon, GRS, codes and their extensions, that are known to be MDS. If $4 \leq n \leq d+1$ and $2 \leq k \leq n-2$, there is linear MDS code of length n and dimension k over $GF(d)$, see [7] for details.

The following result gives many examples of AME states of minimal support. It has been stated in [4] resorting to the theory of linear MDS codes, as referred to above, and in [1] using the theory of orthogonal arrays¹.

Theorem 3 ([4, 1]). *There are $AME(n, d)$ states of minimal support, whenever $n \geq 4$ and $d \geq n-1$ is a power of a prime number.*

Corollary 3. *If d is a prime power, $d \geq 3$, then $\mathcal{N}(d) \geq d+1$.*

¹Due to a typographical error, the result is stated in [1] for a general integer dimension d . The authors meant to state it in the case where d is a prime power.

4 A negative example

Theorem 4. *There is no $AME(7, 5)$ state of minimal support, $\mathcal{N}(5) = 6$.*

Proof. As in [7], define $L_d(k)$ as the maximum wordlength of any linear MDS code of dimension k over $GF(d)$, d being a prime power. Several bounds and equalities are known about $L_d(k)$, see [7]. We will use that $L_d(3) = d + 1$ if d is an odd prime power. In particular, we use that $L_5(3) = 6$.

This shows that no linear MDS code over $GF(5)$ exists with wordlength 7 and dimension 3.

Now suppose that an $AME(7, 5)$ state of minimal support exists. By theorem 1, there is a MDS code over $GF(5)$ with wordlength 7 and minimum distance 5.

The code given in theorem 1 however, is not guaranteed to be linear, so this bound $L_5(3) = 6$ on the theory of linear codes does not suffice to prove the statement.

To end the proof, we note a result of [5], that any MDS code, not necessarily linear, over an alphabet of size 5, code size 5^k , $k \geq 3$, and minimum distance $\delta \geq 3$, can be transformed to a linear MDS code with the same parameters and dimension k with a permutation of coordinates, followed by a permutation of the symbols at each coordinate separately.

This proves that no $AME(7, 5)$ state of minimal support exists and $\mathcal{N}(5) \leq 6$, corollary 3 gives the reverse inequality. \square

The necessary condition given in theorem 2 does not forbid the existence of $AME(7, 5)$ states of minimal support. This necessary condition, therefore, is not sufficient.

5 Conclusions

The existence problem for $AME(n, d)$ states is a non trivial one, even for states minimally supported.

$AME(n, d)$ states of minimal support exist if, and only if $n \leq \mathcal{N}(d)$, and the necessary and sufficient conditions reviewed in this paper can be read as:

$$d + 1 \leq \mathcal{N}(d) \leq 2d - 2, \text{ or } 2d - 3,$$

for $d \geq 3$, the inequality on the right being valid for any integer d and the one on the left being valid for all d power of a prime number. We have seen that the upper bound for $\mathcal{N}(d)$ is not tight, since $\mathcal{N}(5) = 6$.

The theory of linear codes is restricted to the case where the local dimension is a prime power. To investigate other local dimensions, further consideration of general (nonlinear) codes and of combinatorial structures, like orthogonal arrays, seems needed. Sharper estimates on the maximum number of sites $\mathcal{N}(d)$ for which there are AME states of minimal support for a given local dimension d are desirable too.

References

- [1] D.Goyeneche, K. Życzkowski, *Genuinely multipartite entangled states and orthogonal arrays*, Phys. Rev. A **90**, 022316 (2014)
- [2] D.Goyeneche, D. Alsina, J.I. Latorre, A. Riera, K. Życzkowski, *Absolutely maximally entangled states and combinatorial designs*, Phys. Rev. A **92**, 032316 (2015)
- [3] W. Helwig, W. Cui, J.I. Latorre, A. Riera, H. Lo, *Absolute Maximal Entanglement and Quantum Secret*

- Sharing*, Phys. Rev. A **86**, 052335 (2012)
- [4] W. Helwig, W. Cui, *Absolutely Maximally Entangled States: Existence and Applications*, arXiv:1306.2536 [quant-ph]
- [5] J. I. Kokkila, D. S. Krotov and P. R. J. Östegard, *On the classification of MDS codes*, IEEE Trans. Inf. Theory **61**(12), 6485-6492 (2015)
- [6] A.J. Scott, *Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions*, Phys. Rev. A **69**, 052330 (2004)
- [7] R.M. Roth, *Introduction to Coding Theory*, Cambridge University Press, (2006)